

SR
1/3/08

At page 34, line ²⁹35, (through the top of page 35),
change the paragraph to read as follows:

ActiveLINC clients and RATL servers normally exchange unencrypted messages that are susceptible to eavesdropping, especially over a public network. Secure communications is possible through use of 'secure sockets' (SSL) instead of standard TCP/IP connections between ActiveLINC clients and the application servers. SSI, is not yet available on MCP and [[OS22200]] OS2200 systems but secure data transport can still be provided through the use of a redirector as shown in Fig. 10. Connections can be used between the ActiveLINC client and an SSL-capable Web server and normal TCP/IP is used to connect to the application servers over a physically secure local network.